REMARKS

The title of the invention has been amended according to the suggestion of the Examiner.

The Examiner rejected claims 11, 14 and 18 under 35 USC 112, second paragraph for indefiniteness. In response to that rejection, claims 11, 14 and 18 have been amended to remove the indefiniteness as to which network node is being referred to.

Various amendments have been made to the claims voluntarily to emphasize that the invention is practiced in IPSect protocol links.

Several dependent claims have been redrafted into independent form to emphasize various aspects of the invention.

Further, new claims have been added to claim other aspects of the invention. For example, new claims 21 and 22 emphasize that there can be more than one TCP/IP connection within the IPSec protocol link, and that the acknowledgment packet is transmitted separately from the TCP retransmission scheme carried out on these TCP/IP connections.

The Examiner has rejected claims 1-3, 6-8, 11-13, 14-16, 18 and 19 as anticipated by Chiu, U.S. patent 5,526,022. The Examiner has also rejected claims 4, 5 and 17 as obvious over Chiu, 5,526,022 in view of Jorgensen (US patent 6,680,922)

Chiu discloses a method for providing a reliable multicast transmission, i.e., transmission from one source to multiple destinations. Chiu teaches at Col. 4, lines 8-21 that the TCP portion of the TCP/IP protocol establishes reliable communications between end statiosn by causing retransmission of the IP packets in case of uni-cast communication. However, according to Chiu, the TCP/IP retransmission causes problems in implementing a reliable multicast, since each destination station should send an individual acknowledgment message to the source, and thereby the large number of acknowledgment messages from a large number of destinations will flood the source station and the network. Col 4, lines 36 - 52. As a solution to this problem, Chiu teaches

to group the destination computers under a smaller number of "repair head" computers. Instead of sending the ACK and NACK messages to the original source, an individual destination computer sends the ACK or NACK message to the "repair head" computer of a group. The repair head handles the retransmission of data packets to the members of the group. Only the repair head transmit ACK and NACK messages to the original source. Col. 4, lines 53 to Col. 5, line 11.

Jorgensen teaches a virtual private network using a wireless PTMP transmission system which uses IPSec as a method of security encryption. The Examiner asserts that Jorgensen teachs insertion of a byte count header at the sending end on information that is delivered to the IP protocol layer and which is encapsulated as part of the packet. This is true and is found in the following passage from Col. 31, lines 50 et seq.

> At the sending end, TCP puts a byte count header on information that will be delivered to the IP protocol layer and encapsulates it as part of the packet. The receiving end, when it gets packets is responsible for resequencing the packets and ensuring its accuracy. If all of the IP flow is not received correctly, the byte count acknowledgment or nonacknowledgment message can be sent back to the sending end, prompting the sending end to resend the bytes necessary to fill in the remaining portions of the packet flow. TCP buffers additional packets until after resending the nonacknowledged packet.

The receiving end is supposed to re-sequence the packets and ensure the accuracy of the transmission. If not all the packets are received correctly, a byte_count acknowledgement message is sent back to the sending end to prompt the sending end to resend the bytes necessary to fill in the remaining portions of the packet flow. This allows accurate flow control to the byte level.

An object of the present invention is to obtain information of the performance of the IPSec link or links in order to be able to select the IPSec link or links, such as the IpSec link with the best performance among several or a plurality of IPSec links available between a source network node and a destination network node.

Chiu fails to provide between a source network node and a destination network node a communication link employing the IPSec protocol for tunnelling IP packets between the source network node and the destination network node. On the contrary, Chiu teaches a multicast transmission from a source network node to multiple destination nodes. Chiu mentions IPSec technology as a possible way to perform sender authentication (Col. 35, lines 34 to 36) but specifically states that the protocols

describede in the Chiu patent do not support such a possibility. **Thus, not only does Chiu not anticipate the amended claims which have been amended to recite use of the IPSec protocol but also teaches away from its use.**

More specifically, Chiu et al. fail to teach or suggest that performance or throughput of the IPSec communication link between a source network node and a destination network node should be monitored or can be monitored. In Chiu, the reliable multicast transmission is achieved by means of the TCP protocol. Chiu explicitly states that the TCP portion of the TCP/IP protocols establishes reliable communications between the source and destination stations by causing retransmission of packets using the IP protocol. The same reliable TCP protocol is utilized in the multicast with the exception that the adknowledgments are transmitted to and the retransmissare are carried out by multiple repair heads in the network.

One fundamental difference between IPSec link protocol and the TCP connection protocol is that a plurality of TCP connections may be transmitted within one IPSec "connection" or tunnel. As explained in the background section of the present patent application at page 2, lines 7-9, "IPSec does not provide flow control or error recovery, but leaves these to the protocols carried within the secured channel created by IPSec."

Therefore, the invention is not an alternative to normal TCP flow control or TCP error recovery based upon retransmission of IP packets. Instead, it is a new way of monitoring IPSec connections for important characteristics such as throughput, operability, round trip transit time, etc.

The present invention does not relate to traditional flow control mechanisms which are used in the connections transmitted inside IPSec tunnels or links. Instead, the claimed invention is specially needed when an IPSec tunnel from node A to node B can be established via more than one internet service provider (ISP) links. The invention provides, *inter alia*, a way to choose between multiple links when multiple links are available.

Chiu Does Not Anticipate The Amended Claims

Chiu does not anticipate the amended claims. For example, amended claim 1 calls for employing the IPSec protocol to tunnel IP packets between the source network node and the destination network node. Chiu does not teach this so amended claim 1 is not anticipated. Amended claim 2 is an independent claim which calls for employing the IPSec protocol for tunnelling IP packets between a source and destination node so it also

is not anticipated. The next independent claim is claim 8. Amended claim 8 calls for employing the IPSec protocol for tunnellin IP packets between the source and destination network nodes and is not anticipated. Claim 9 calls for monitoring an active communication link employing the IPSec protocol and calls for the monitoring to be carried out using transmissions of acknowledgment packets by the destination network node after either a predetermined number of IPSec packets have been received or a packet is received after a timeout from transmission of the last acknowledgment packet. The monitoring of an IPSec link is not taught in Chiu et al. The next independent claim is 11. That claim is an apparatus claim which calls for communicating over an IPSec protocol communication link to tunnel IP packets transmitted to a second network node. The next independent claim is claim 13. That claim, as amended, calls for means for communicating over an IPSec protocol communication link to tunnel IP packets to a second network node. Again, this element is not anticipated by Chiu et al. The same is true of original independent claims 14, 15, 18 and 19 all of which have been amended to add this same element not found in Chiu et al. The same is true of new independent claims 20 and 21 all of which have been written to include use of the IPSec protocol to tunnel IP packets to a second node as part of the claimed invention. This element is not present in Chiu et al. so these claims are not anticipated.

Further, in view of the specific teachings of Chiu, there would have been no motivation for a person skilled in the art to monitor the performance or throughput of the IPSec link on the IPSec level in addition to the TCP flow control and error recovery even in the case where IPSec protocol had been employed between the sender and the destination. Chiu explicitly teaches that TCP is sufficient for providing reliable communication. On the contrary, the skilled person would have considered any additional signalling in the network as a detriment since the Chiu primarily seeks a solution for decreasing the signalling load. As such, Chiu et al. teaches away from the invention.

Moreover, Chiu fails to teach or suggest monitoring of an IPSec link by means of transmitting acknowledgment packets by the destination network node if at least one of the first condition or the second condition is fulfilled, as defined in claim 1.

Chiu further fails to teach that the first condition is the reception of at least a predetermined number of IPSec packets after transmission of the previous acknowledgment packet.

The Examiner refers to col. 16, lines 63-67 as disclosing the first condition. This

passage from Chiu refers to a TCP acknowledgement window for the TCP error recovery. Chiu fails to teach to count the number of IPSec packets after transmission of the previous acknowledgement packet.

The Examiner further refers to col. 17, lines 7-15 as disclosing the second condition. This section of Chiu teaches to send a TCP acknowledgement, if no IP packets have been received from the sender within the set period of time. This relates to a situation in which the sender has paused.

In the present invention, the second condition is totally different: an acknowledgement packet is transmitted if an IPSec packet is received via the communication link after the predetermined time has passed after transmission of a previous acknowledgement packet.

For the foregoing reasons, the claimed invention is new and is not obvious over Chiu.

Regarding claims 2, 11 and 19, Chiu further fails to teach that the acknowledgement comprises at least the sequence number of the last received IPSec packet and at least a value corresponding to the amount of data received via the IPSec communication link.

The Examiner refers to Column 17, lines 21-42. Chiu teaches that the TCP acknowledgement message includes a sequence number that indicates the first missing TCP packet. This is totally different from the claimed feature in which the sequence number of the last received IPSec packet is indicated. In Chiu, the acknowledgment includes also a bit map that indicates which data packets are missing starting from the sequence number indicated in the acknowledgement. This bit map indicates which data packets must be retransmitted and is used for this purpose. There is no teaching or suggestion that the bitmap would be used to indicate the amount of data received.

The Examiner also refers to Col. 37, lines 35-55 and Col. 38, lines 1-7 as disclosing that the send can calculate the total size of data that is being transferred. This value is calculated in order to be able to further determine the average rate of data transmission to be used. Chiu fails to teach that this value would be used with the bit map for determining the success rate and throughput from the sender to an individual receiver. Actually, the bit map of an individual receiver is never forwarded to the original sender in the system of Chiu. The sender adjusts the transmission rate according to the overall congestion status in the network.

Further, the specific sections in Chiu cited by the Examiner relate to the TCP retransmission scheme of IP packets, and are not related to the monitoring of an IPSec communication link as in the present invention.

Regarding claims 8 and 13, Chiu fails to teach storing the sequence number and the transmission time of each IPSec packet transmitted from the source network node to the destination network node in a memory means and determining the roundtrip time of the communication link on the basis of a reception time of an acknowledgement packet and the stored transmission time of the corresponding transmitted packet.

The Examiner refers to Col. 3, lines 51-54, as well as Col. 12, lines 65-67 and Col. 13, lines 1-7. The IP packets are naturally stored for retransmission purposes by the sender. However, no transmission time is stored when each packet is transmitted. Col. 12, line 65 to Col. 13, line 7 merely discloses a rate adaptation at the transmitter based on the targeted average transfer rate. No reception time of the acknowledgement packet from an individual receiver is determined. Therefore, there are no stored transmission times and no determined reception times that are available in the Chiu et al. system which are available to calculate roundtrip transmission times for individual communication links. In accordance with the principles of Chiu, an acknowledgement from an individual receiver will never be forwarded to the original sender, in order to avoid overloading the sender since Chiu teaches a point-to-multipoint system for multicast.

Further, the specific disclsosure in Chiu relates to the TCP retransmission scheme for TCP packets, and is not related to the IPSec packets and IPSec link as in the present invention as claimed.

The Examiner rejected claims 4, 5 and 17 as being unpatentable as obvious over a combination of the teachings of Chiu et al. in view of Jorgensen. These claims are dependent claims which depend from independent claims 2 and 15. As discussed above, Chiu fails to teach or suggest the subject matter of these independent claims. Further, as the Examiner admits, Chiu fails to disclose that the acknowledgement packet comprises the byte counter value indicating the number of bytes received via a communication link.

The Examiner refers to Col. 46, lines 6-9, and Col 31, lines 50-61 in Jorgensen. Jorgensen teaches that the TCP protocol of the sender provides an IP packet with a byte number that can be used for indication and retransmission of missing bytes in a packet

flow. This corresponds to the IP sequence number.

However, this is not a byte counter value provided by the receiver and indicating the number of bytes received via the communication link as claimed in claims 4, 5 and 17.

The Examiner also rejected claims 9 and 10 as obvious over a combination of Chiu et al. and Tam (US patent 6,622,172). As already discussed above, Chiu fails to teach or suggest the features disclosed on lines 1-15 in claim 9.

Further, as admitted by the Examiner, Chiu fails to teach the monitoring of an inactive communication link as disclosed in claim 9.

The Examiner refers to Col. 11, lines 45-60 and Figure 2 in Tam as disclosing these features of monitoring of an inactive communication link. However, Tam teaches probing of a TCP communication protocol link and not an IPSec communication link. Tam fails to teach monitoring an inactive IPSec link between a source network node and a destination network node having an active IPSec link that is monitored at the same time.

Further, Chiu and Tam fail to teach or suggest to maintain present status of active and inactive IPsec communication links or replacing said active communication link with said inactive communication link based on results of said monitoring, as claimed in claim 9. Further, regarding claim 9, Chiu and Tam fail to teach determining , in addition to the roundtrip time of said inactive communication link, als the packet success rate of the inactive communication link. Therefore, claims 9 and 10 are not obvious from Chiu in view of Tam.

Favorable action is ernestly solicited.

Respectfully submitted,

Dated: July 8, 2004

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.

on 7/8/04
(Date of Deposit)

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843